



Docket No.: SONY-50R4813

Patent *IFW*

I hereby certify that this transmittal of the below described document is being deposited with the United States Postal Service in an envelope bearing First Class Postage and addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date of deposit.

Date of Deposit:	05/29/07	Name of Person Making the Deposit:	Julie Giaramita	Signature of the Person Making the Deposit:	<i>Julie Giaramita</i>
------------------	----------	------------------------------------	-----------------	---	------------------------

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Iwamura

Application No.: 09/972,371

Examiner:

Filed: 10/05/01

Art Unit:

For: METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER WITH SECURE KEY DISTRIBUTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Sir:

Transmittal of an Appeal Brief
(Under 37 CFR §1.192)

☒ Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on: 03/26/07

X The application is on behalf of other than a small entity

..... The application is on behalf of a small entity.

..... A verified statement of small entity status is attached.

..... A verified statement of small entity status has been previously filed herein.

Fee Calculation (for other than a small entity)

Filing Appeal Brief	\$500	\$500.00
Total Fees		\$500.00

PAYMENT OF FEES

1. The full fee due in connection with this communication is provided as follows:

[X] The Commissioner is hereby authorized to charge any additional fees associated with this communication or credit any overpayment to Deposit Account No.: 50-4160.
A duplicate copy of this authorization is enclosed.

[X] A check in the amount of \$500.00

[] Charge any fees required or credit any overpayments associated with this filing to Deposit Account No.: 50-4160.

Please direct all correspondence concerning the above-identified application to the following address:

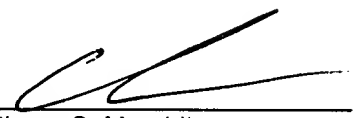
MURABITO HAO & BARNES LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

Respectfully submitted,

Date:

5/29/2007

By:


Anthony C. Murabito
Reg. No. 35,295



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant: Iwamura Patent Application
Serial No.: 09/972,371 Group Art Unit: 2132
Filed: October 5, 2001 Examiner: Benjamin E. Lanier
For: METHOD AND SYSTEM FOR A SECURE DIGITAL
DECODER WITH SECURE KEY DISTRIBUTION

Appeal Brief

06/04/2007 AAHHADI 00000009 09972371

01 FC:1402

500.00 0P

Table of Contents

	<u>Page</u>
Real Party in Interest	1
Related Appeals and Interferences	2
Status of Claims	3
Status of Amendments	4
Summary of Claimed Subject Matter	5
Grounds of Rejection to be Reviewed on Appeal	8
Arguments	9
Conclusions	29
Claims Appendix	30
Evidence Appendix	35
Related Proceedings Appendix	36

Real Party in Interest

The assignee of the present invention is Sony Electronics, Inc.



SONY-50R4813/ACM/NAO

Serial No.: 09/972,371
Group Art Unit: 2132

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-7 and 17-20 are pending. Claims 17-20 are rejected under 35 USC § 102(e). Claims 1-7 are rejected under 35 USC § 103(a).

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the final rejection has not been filed.

Summary of Claimed Subject Matter

One embodiment of the present claimed invention pertains to a method for securely decrypting and decoding a digital signal. One embodiment of the present invention first accesses an encrypted signal at a first logical circuit. Next, this embodiment determines a broadcast encryption key for the encrypted signal at a second logical circuit separate from the first logical circuit. For example, the second logical circuit where the broadcast key was determined may be across a communication link from the first circuit where the signal is being received. Then, the broadcast encryption key is encrypted by means of a public key and transferred over the communication link. Next, at the first logical circuit, the encrypted broadcast encryption key is decrypted. Therefore, the broadcast encryption key is determined. Then, at the first logical circuit, the encrypted signal is decrypted using the broadcast encryption key. Consequently, the encrypted signal is decrypted without exposing the broadcast encryption key on the communication link in an un-encrypted form.

Independent Claim 1 recites:

A method of securely processing a digital signal comprising:

a) generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit;

in a digital media receiving device:

- b) accessing an encrypted signal at said first logical circuit;
- c) determining a first decryption key for said encrypted signal at said second logical circuit;
- d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;
- e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;
- f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key; and
- g) at said first logical circuit, decrypting said encrypted signal using said first decryption key.

Figures 2, 3A, 3B and 6 of the instant specification illustrate hardware embodiments of the present invention, upon which a method embodiment of Claim 1 may be practiced, in accordance with this Claim. Figure 4 illustrates a method embodiment of Claim 1. Explanation of these items is provided by the instant Specification at least at page 12 line 14 *et. seq.*, page 14 line 21 *et. seq.*, page 17 line 4 *et. seq.*, page 24 line 4 *et. seq.*, and page 18 line 11 *et. seq.*, *inter alia*.

Independent Claim 17 recites:

A system for processing a secure digital signal, comprising:
in a digital media receiving device:

a first logical circuit for decrypting a local encryption key, said first logical circuit comprising a local processor and local memory; and
a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit.

Items 333 and 335 of Figure 3A illustrate embodiments of the present invention in accordance with this Claim. Explanation of these items are provided by the instant Specification at least at page 14 line 21 *et. seq., inter alia*.

Grounds of Rejection to be Reviewed on Appeal

Appellants appeal the rejection of Claims 17-20 under 35 USC § 102(e) as allegedly unpatentable over Johnston (US 6,373,946, "Johnston").

Appellants appeal the rejection of Claims 1 and 3-7 under 35 USC § 103(a) as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo").

Appellants appeal the rejection of Claim 2 under 35 USC § 103(a) as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo") and further in view of Schneier (Applied Cryptography, 1996, John Wiley & Sons, pp 513-514, "Schneier").

Arguments

A. Rejection of Claims 17-20 under 35 USC § 102(e) as allegedly unpatentable over Johnston (US 6,373,946, “Johnston”)

Appellants respectfully assert that Johnston fails to teach or suggest the claimed limitation of “a digital media receiving device,” as recited by Claim 17. Appellants respectfully assert that one of ordinary skill in the art would not understand the taught voice-only system of Johnston to teach or suggest “digital media” as recited by Claim 17. For example, a voice-only telephone is not generally known as or referred to as a “media device.” Simply using digital technology to implement a telephone for voice communication likewise does not make it a “digital media device” as understood by those of ordinary skill in the art.

For this reason, Appellants respectfully assert that Claim 17 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

In addition with respect to Claim 17, Appellants respectfully assert that Johnston fails to teach or suggest the claimed limitation of a “receiving device,” as recited by Claim 17. Appellants respectfully assert that one of ordinary skill in the art would not understand the taught telephone to be a

“receiving” device. For example, transmission is fundamental to the operation of such a telephone. Appellants respectfully assert that one of ordinary skill in the art would understand the recited receiving device to be a device that primarily functions to receive. In contrast, the taught telephone has a primary function of two-way communication.

For this additional reason, Appellants respectfully assert that Claim 17 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Further still with respect to Claim 17, Appellants respectfully assert that Johnston fails to teach or suggest the claimed limitation of “encrypting said digital signal” in a receiving device, as recited by Claim 17. While Johnston may teach encrypting, such encrypting is taught “for data to be transmitted” (column 10, line 53, *inter alia*, emphasis added). Johnston fails to teach or suggest encrypting data on reception as claimed. Claim 17 recites encryption in a receiver. While Johnston may teach encryption in a transmitter, Appellants respectfully assert that Johnston fails to teach or suggest the instant limitation of encryption in a receiver.

For this further still reason, Appellants respectfully assert that Claim 17 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Moreover, Johnston actually teaches decryption of a received signal (column 11, lines 4-5), in contrast to embodiments in accordance with Claim 17 that recite encryption of a received signal. In this manner, Johnston actually teaches away from embodiments in accordance with the present invention as recited by Claim 17.

For this further yet reason, Appellants respectfully assert that Claim 17 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Appellants respectfully assert that Claims 18-20 overcome the rejections of record by virtue of their dependency, and respectfully submit that these Claims are patentable.

Further with respect to Claim 19, Appellants respectfully assert that Johnston fails to teach or suggest the claimed limitation, “a modifiable local memory contained within said first logical circuit, said modifiable local

memory enabling the modification of a computer control program stored within said local memory” as recited by Claim 19.

Johnston teaches, “the subscriber has no access to the data stored in the SIM” (column 1 lines 36-37). Appellants respectfully assert that the taught “no access” teaches away from the instant limitation.

For this further reason, Appellants respectfully assert that the rejection of Claim 19 is overcome, and respectfully submit that this Claim is patentable.

Further still with respect to Claim 19, the rejection cites Johnston column 16 lines 47-49 as suggesting the limitations of this Claim. Appellants respectfully traverse. Appellants understand the cited passage to refer to replacement of SIM cards to enable secure communications among a group. For example, SIM cards with different characteristics are “provided” to “all user terminals” (column 16 lines 30-49, emphasis added). Neither the cited passage nor the whole of Johnston teaches or suggests modification of a SIM card. Even if, *arguendo*, Johnston suggests modification of a SIM card, Johnston fails to suggest that such modifications take place within said “digital media receiving device,” as recited by Claim 19.

For this further still reason, Appellants respectfully assert that the rejection of Claim 19 is overcome, and respectfully submit that this Claim is patentable.

B. Rejection of Claims 1 and 3-7 under 35 USC § 103(a) as allegedly unpatentable over Spies et al. (US 6,055,314, "Spies") in view of Deo et al. (US 5,721,781, "Deo")

The rejection proposes to modify Spies in view of Deo. However, Doe teaches an authentication system that is dependent upon hardware comprising global secrets, e.g., digital certificates (Abstract). In contrast, Spies specifically teaches away from such a system. "It is therefore another object of this invention to provide a ... system that has no global secrets built into any hardware..." (Spies, column 2 lines 1-5). Consequently, Appellants respectfully assert that one of ordinary skill in the art would be taught away from the proposed modification of Spies in view of Deo in view of the teachings of Spies. There is therefore no suggestion in the cited art to combine the references to realize the claimed embodiments.

For this reason, Appellants respectfully assert that Claims 1 and 3-7, and all other claims rejected over a combination of Spies in view of Deo, overcome the rejections of record, and respectfully submit that these Claims are patentable.

Importantly, Appellants respectfully assert that the proposed combination of Spies in view of Deo would change a principle of operation of

at least one of the references. It is well held that if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious (*In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)).

Doe teaches, “the cardholder enters a unique PIN into the terminal” as a part of a “three-tiered authentication system” (Abstract, *inter alia*).

Entering a PIN code into a digital media receiving device is not taught by Spies, and would be understood by one of ordinary skill in the art to be an undesirable encumbrance to the usability of the recited digital media receiving device. For example, entering a PIN into an automatic teller machine (ATM) is common; however, entering a PIN into a set top box is unknown to the Appellants. Appellants respectfully assert that requiring a viewer to enter a PIN into the recited digital media receiving device would be an undesirable detriment to usability and market acceptance of such a device.

As the taught “three-tiered authentication system” is fundamental to Deo, removal of the PIN requirement for the proposed combination inherently changes at least one principle of operation of Deo. If the proposed

combination retains Deo's PIN requirement, such combination inherently changes at least one principle of operation of Spies.

As the proposed modification would change a principle of operation of at least one of the references, Appellants respectfully assert that the proposed modification of Spies in view of Deo renders an improper combination under 35 USC § 103. For this additional reason, Appellants respectfully assert that Claims 1 and 3-7, and all other claims rejected over a combination of Spies in view of Deo, overcome the rejections of record, and respectfully submit that these Claims are patentable.

Appellants respectfully assert that the rejection's citation of Deo is improper because the reference is nonanalogous art per *In re Clay*, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). Appellants understand Deo to be directed to "portable information devices such as smart cards, personal digital assistants, pagers, and other personal information managers, and the mechanisms used to access these devices."

Appellants respectfully assert that Doe would not commend itself to one of ordinary skill in the art in consideration of the problems solved by the present invention, due to the myriad well known differences between the taught "portable information devices" and the recited digital media receiving devices. For example, one of ordinary skill in the art would not consider a

“Point of Deployment security module (POD)” as commonly used with digital media receiving devices to be analogous with the taught “portable information devices.” In fact, many deployments of PODs include contractual agreements prohibiting removal of the POD from the digital media receiving device. Further, some digital media receiving devices include means to prevent or discourage removal of a POD, including, e.g., erasure or destruction of the POD responsive to attempted removal. Thus, POD devices are, by design and operation, not “portable.”

In consideration of such differences, Appellants respectfully assert that one of ordinary skill in the art in consideration of the problems solved by the present invention would not be motivated to utilize the non-analogous teaching of Deo.

For this further reason, Appellants respectfully assert that Claims 1 and 3-7, and all other claims rejected over Deo, alone or in combination, overcome the rejections of record, and respectfully submit that these Claims are patentable.

With respect to Claim 1, Appellants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the claimed limitation “at said first

logical circuit, decrypting said encrypted signal using said first decryption key” as recited by Claim 1.

In contrast, Spies teaches, “[t]he view computing unit 60 is not permitted, however, to read the decryption capabilities” (column 9, lines 25-26, emphasis added) and “the individual packet keys are never made available to the viewer computing unit...” (column 10, lines 46-47, emphasis added). Thus, in accordance with the teaching of Spies, the recited “first logical unit” does not decrypt the accessed encrypted signal, and further does not decrypt the accessed encrypted signal using the recited “first decryption key.”

In teaching benefits of keeping decryption capabilities and packet keys solely within the IC card, Spies actually teaches away from embodiments of the present invention that recite transferring a decryption key.

While the proposed modification of Spies in view of Doe is alleged to teach encryption and decryption of the recited first decryption key, Appellants respectfully assert that such teaching, *even if present*, does not remedy this deficiency of Spies, nor does the rejection allege that it does.

For these reasons, Appellants respectfully assert that Claim 1 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

The rejection argues, “the CPU of the set top box (first logical unit) receives the decryption key from the IC card to decrypt the encrypted signal.” Appellants respectfully assert that such a teaching fails to teach or suggest embodiments of the present claimed invention as recited in Claim 1.

Claim 1 recites, in part, the following limitations:

- d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;
- e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;
- f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key

Appellants respectfully assert that Spies fails to teach or fairly suggest the recited limitations of encrypting a decryption key, transferring the encrypted encryption key to another logical unit, and decrypting the encrypted decryption key.

Deo fails to remedy this deficiency of Spies as Deo fails to teach or fairly suggest use of the digital certificate exchange technique for uses other than certificate exchange.

For this additional reason, Appellants respectfully assert that Claim 1 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Appellants respectfully assert that Claims 2-7 overcome the rejections of record by virtue of their dependency, and respectfully solicit allowance of these Claims.

In addition with respect to Claim 4, Appellants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation “replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program” in conjunction with the other limitations as recited by Claim 4.

While Spies may teach that cryptographic service providers (CSPs) can be changed or updated, Spies does not teach a method or system for such updates. In particular, Spies teaches such CSPs are “preferably ... stored in ROM (read only memory)” (column 11 lines 64-66). Appellants respectfully

assert that one of ordinary skill in the art would understand that changing software stored in a ROM requires physical replacement of the ROM device. Moreover, software “stored in ROM” cannot be replaced as recited by Claim 4, as a ROM is, by definition, not writable. Consequently, Spies fails to teach updating software within the operation of the media system, as recited by Claim 4.

Deo is not alleged to correct this deficiency of Spies, and Appellants respectfully assert that it does not.

For these additional reasons, Appellants respectfully assert that Claim 4 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

In addition with respect to Claim 6, the rejection of February 17, 2006, concedes, “[r]eferring to claim 6... Spies and Deo do not disclose decryption routine can be updated/replaced.” A third piece of art, not cited in the present rejection, was introduced in the rejection of Claim 6. As the rejection of February 17, 2006 concedes that Spies and Deo are not sufficient to reject Claim 6, Appellants respectfully assert that Claim 6 overcomes the rejections of record, and respectfully solicit allowance of this Claim.

In addition with respect to Claim 7, Appellants respectfully assert that Spies in view of Deo fails to teach or fairly suggest the limitation “wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format” as recited by Claim 7.

While Spies may teach the “video content can be TV broadcasts” as stated in the rejection, Appellants respectfully assert that the recited signal is not limited to “TV broadcasts” or even to video. For example, it is well known that compact disc (CD) audio is digital; however, it is generally not encoded in MPEG.

Moreover, the cited references do not teach or fairly suggest MPEG compliant signals. Both references are completely silent as to MPEG.

The rejection cites, but does not rely on, Walkinson, “The MPEG Handbook,” 2004, Focal Press, Second Edition, Pages 366-381, 389-394 (“MPEG”). Appellants are confused by the rejection’s treatment of this reference. MPEG shows a publication date of 2004, which is significantly later than the priority date of the present application (2001). Even, *arguendo*, using the earliest copyright date of 2001 listed for the non-cited first edition of MPEG, MPEG does not appear to qualify as § 102(b) prior art,

as MPEG was published less than one year prior to the priority date of the present application (2001).

As MPEG is not applied in the rejection, and MPEG does not qualify as statutory prior art, Appellants respectfully assert that Claim 7 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

In addition with respect to Claim 7, the rejection appears to allege that Spies is directed only to digital distribution of video content, and that the MPEG reference teaches all digital video is MPEG encoded. Appellants respectfully traverse both allegations. Spies is directed to “purchase and delivery of video content programs over various distribution media” (Abstract, emphasis added). Appellants do not find Spies to exclude non-digital distribution. For example, Spies lists “video cassettes” (column 1 lines 15-16) as a common means of distributing video content. Appellants respectfully assert that the major video tape formats (e.g., VHS) are neither encoded in a digital format nor are a digital distribution media. Consequently, Spies is not limited to only digital distribution.

Further, Spies teaches, “[v]ideo content programs are commonly supplied to viewers in many different forms, including theater films, video cassettes, TV cable and broadcast systems, game CDs, and on-line networks”

(column 1 lines 14-17). Appellants respectfully assert that it is well known that the taught “theater films (and) video cassettes” are non-digital media. Appellants respectfully assert that it is well known that the taught “TV cable and broadcast systems” may be non-digital, and in fact the majority of such systems, including over-the-air broadcast television, are non-digital.

Therefore, *arguendo*, if the rejection’s allegation that all digital video is MPEG encoded, it does not follow that Spies suggests such encoding, as Spies allows for non-digital distribution.

For this additional reason, Appellants respectfully assert that Claim 7 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Further with respect to Claim 7, Appellants traverse the rejection’s finding that all digital video is inherently MPEG encoded. Spies teaches that video content program distribution media may include “game CDs” and “on-line networks.” Appellants respectfully assert that the taught “game CDs” and “on-line networks” may use non-MPEG encoding. For example, Audio Video Interleave (“AVI”) encoding is widely used in the taught “on-line networks.” As it is obviously possible to use non-MPEG methods to encode digital video, MPEG is not inherent. Consequently, the rejection’s allegation

of inherency is improper, and any rejections that rely upon such an allegation are overcome.

For this further reason, Appellants respectfully assert that Claim 7 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

C. Rejection of Claim 2 under 35 USC § 103(a) as allegedly unpatentable over Spies et al. (US 6,055,314, “Spies”) in view of Deo et al. (US 5,721,781, “Deo”) and further in view of Schneier (Applied Cryptography, 1996, John Wiley & Sons, pp 513-514, “Schneier”)

Appellants respectfully assert that Claim 2 overcomes the rejections of record as Spies teaches away from a combination with Deo, for the rationale previously presented in Argument B, and respectfully submit that this Claim is patentable.

Appellants respectfully assert that Claim 2 overcomes the rejections of record by virtue of its dependency, and respectfully submit that this Claim is patentable.

Further with respect to Claim 2, Appellants respectfully assert that Spies actually teaches away from embodiments of the present invention that recite the limitation of “generating said public encryption key using the technique of Diffie-Hellman Key Exchange” as recited by Claim 2.

In contrast, Spies teaches, “[t]he view computing unit 60 is not permitted, however, to read the decryption capabilities” (column 9, lines 25-26, emphasis added) and “the individual packet keys are never made

available to the viewer computing unit...” (column 10, lines 46-47, emphasis added). Thus, in accordance with the teaching of Spies, the recited “first logical unit” does not decrypt the accessed encrypted signal, and further does not decrypt the accessed encrypted signal using the recited “first decryption key.”

Thus, Spies teaches away from key exchange.

Doe fails to remedy this deficiency of Spies. Doe teaches “authentication” of a smart card and an ATM based upon the well known technique of certificate exchange. Accordingly, Doe depends upon a trusted third party, a “certifying authority” (column 7, lines 45-60). Further, Doe teaches transfer of keys via “certificates,” e.g., “the smart card uses the terminal’s public key that it received in the terminal’s certificate” (column 7, lines 1-3).

By teaching trust in a third party “certifying authority” and by teaching transfer of keys via certificates, Doe actually teaches away from “generating said public encryption key using the technique of Diffie-Hellman Key Exchange” as recited by Claim 2.

For these further reasons, Appellants respectfully assert that Claim 2 overcomes the rejections of record, and respectfully submit that this Claim is patentable.

Conclusions

Appellants believe that pending Claims 1-7 and 17-20 are patentable over the cited art. Appellants respectfully request that the rejection of these claims be reversed.

Date: _____

5/29/2007

Respectfully submitted,

MURABITO, HAO & BARNES LLP



Anthony C. Murabito
Reg. No. 35,295

Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060

Claims Appendix

1. (previously presented) A method of securely processing a digital signal comprising:

a) generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit;

in a digital media receiving device:

b) accessing an encrypted signal at said first logical circuit;

c) determining a first decryption key for said encrypted signal at said second logical circuit;

d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;

e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;

f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key; and

g) at said first logical circuit, decrypting said encrypted signal using said first decryption key.

2. (original) The method of Claim 1 wherein a) comprises generating said public encryption key using the technique of Diffie-Hellman Key Exchange.

3. (original) The method of Claim 1 wherein d) comprises:

SONY-50R4813/ACM/NAO

Serial No.: 09/972,371
Group Art Unit: 2132

d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) accessing a computer control program from a second portion of local memory at said second logical circuit; and

d3) executing said computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

4. (original) The method of Claim 1 wherein d) comprises:

d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program;

d3) accessing said new computer control program from said second portion of local memory; and

d4) executing said new computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

5. (original) The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) accessing a computer control program from a second portion of local memory at said first logical circuit; and

f3) executing said computer control program to decrypt said first decryption key using said second decryption key.

6. (original) The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) replacing a computer control program stored in a second portion of local memory at said first logical circuit with a new computer control program;

f3) accessing said new computer control program from said second portion of local memory; and

f4) executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

7. (original) The method of Claim 1 wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format.

8-16 (canceled) (election)

17. (previously presented)A system for processing a secure digital signal, comprising:

in a digital media receiving device:

a first logical circuit for decrypting a local encryption key, said first logical circuit comprising a local processor and local memory; and

a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit.

18. (original)The system of Claim 17, further comprising a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

19. (original)The system of Claim 17, further comprising a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

20. (original)The system of Claim 17, further configured such that the contents of said local memory cannot be observed from outside of said first logical circuit.

21-25 (canceled) (election)

Evidence Appendix

None.

Related Proceedings Appendix

None.